(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 21 484 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 L 12/28
H 04 M 1/66
H 04 M 3/22
H 04 M 11/00

(21) Aktenzeichen: 195 21 484.6
(22) Anmeldetag: 13. 6. 95
(43) Offenlegungstag: 19. 12. 96

DE 195 21 484 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

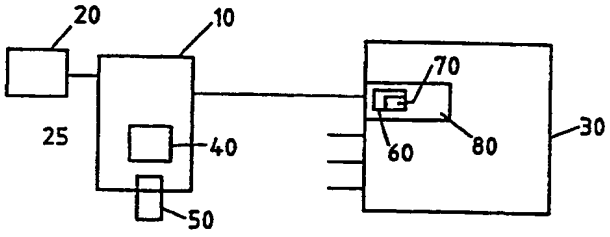
(72) Erfinder:
Stolz, Helmut, Dipl.-Ing., 57080 Siegen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 43 39 460 C1
DE 39 19 734 C1
DE 44 06 602 A1
DE 43 35 161 A1
DE 41 38 861 A1
DE 41 20 398 A1
DE 39 05 667 A1
DE 94 17 399 U1
FR 26 19 941 A1
US 53 57 563
US 53 07 411
US 52 97 192
US 50 36 461
EP 06 18 713 A2
PRESTTUN,K.: Sicherungsfunktionen in Nachrichtennetzen. In: Elektrisches Nachrichtenwesen, Bd.60, Nr.1, 1986, S.63-70;
SCHULTE,Heinz: Telekommunikation, Bd.3, Loseblattsammlung, Interest Verlag GmbH, Augsburg, 1988, Teil 13, Kapitel 2.6, S.9-23;

(54) Verfahren und Vorrichtung zur Authentisierung von Teilnehmern gegenüber digitalen Vermittlungsstellen

(57) Die Erfindung betrifft ein Verfahren zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen eines digitalen Kommunikationsnetzwerkes, insbesondere ein ISDN-Netz, gemäß Anspruch 1 sowie eine Vorrichtung zur Authentisierung von Teilnehmern gemäß den Ansprüchen 6 und 8. Da die Verbindungswege zwischen Teilnehmeranschlüssen und der Vermittlungsstelle nicht gesichert sind, besteht die Gefahr, daß Eindringlinge bzw. Lauscher diese Verbindungswege abhören können.
Der Erfindung liegt daher die Aufgabe zugrunde, einen Mißbrauch der Vermittlungsstelle durch einen nichtberechtigten Eindringling zu erschweren oder sogar völlig zu beseitigen. Dazu schafft die Erfindung eine Vorrichtung zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen eines digitalen Kommunikationsnetzes mit wenigstens einer teilnehmerseitigen Netzabschlußeinrichtung, an die wenigstens eine Datenendeinrichtung anschaltbar ist. Die Erfindung zeichnet sich dadurch aus, daß bei jedem Teilnehmer wenigstens ein erstes Authentisierungsmodul angeordnet ist, das einen ersten Identitätsträger aufnehmen kann, daß in der Vermittlungsstelle wenigstens ein zweites Authentisierungsmodul angeordnet ist, das einen zweiten Identitätsträger aufnehmen kann, oder daß alternativ zwischen die der Vermittlungsstelle zugeordneten Netzabschlußeinrichtungen und die Vermittlungsstelle eine Zusatzeinrichtung geschaltet ist, in der wenigstens ein zweites Authentisierungsmodul ...



DE 195 21 484 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen eines digitalen Kommunikationsnetzwerkes, insbesondere ein ISDN-Netz, gemäß Anspruch 1 sowie eine Vorrichtung zur Authentisierung von Teilnehmern gemäß den Ansprüchen 6 und 8.

Es sind digitale Kommunikationsnetze bekannt, die über mehrere Teilnehmeranschlüsse und digitale Vermittlungsstellen verfügen. Da ein Teilnehmeranschluß über nicht gesicherte Verbindungswege an eine digitale Vermittlungsstelle angeschlossen wird, können Eindringlinge oder sogenannte Lauscher die Verbindungswege abhören, indem sie sich an verschiedenen Punkten in bestehende Verbindungswege einschalten bzw. auf die bestehenden Verbindungswege aufschalten. Hat sich ein Eindringling auf diese Weise erst einmal Zugang zum Vermittlungssystem verschafft, kann er, obwohl er nicht authorisiert ist, die Vermittlungsstelle auf Kosten des Anschlußinhabers benutzen.

Der Erfindung liegt daher die Aufgabe zugrunde, einen Mißbrauch der Vermittlungsstelle durch einen nicht berechtigten Eindringling zu erschweren oder sogar völlig zu beseitigen.

Die Erfindung löst diese Aufgabe durch die Schritte des Verfahrensanspruchs 1 sowie durch die Merkmale der Vorrichtungsansprüche 6 und 8.

Die Erfindung ist in einem digitalen Kommunikationsnetz, insbesondere dem ISDN-Netz, verwirklicht. Ein derartiges digitales Kommunikationsnetz umfaßt bekannterweise mehrere Vermittlungsstellen, wenigstens eine beim Teilnehmer installierte Netzabschlußeinrichtung, an die wenigstens eine Datenendeinrichtung, beispielsweise Telefongeräte, Personalcomputer oder Facsimilegeräte, anschaltbar ist. Eine ungewollte Benutzung einer Vermittlungsstelle durch einen Eindringling wird nun dadurch verhindert, daß bei jedem Inhaber eines Teilnehmeranschlusses wenigstens ein erstes Authentisierungs-Modul angeordnet ist, das einen Identitätsträger aufnehmen kann, daß darüber hinaus in der Vermittlungsstelle wenigstens ein zweites Authentisierungs-Modul angeordnet ist, das einen zweiten Identitätsträger aufnehmen kann, wobei die beiden Authentisierungs-Module Informationen mit einem teilnehmerspezifischen, kryptographischen Schlüssel zur einseitigen und/oder gegenseitigen Authentisierung ver- und/oder entschlüsseln und die Informationen untereinander austauschen können.

In jeder Vermittlungsstelle sind anschlußspezifische Baugruppen eingebaut, die jeweils das zweite Authentisierungs-Modul enthalten. Diese Ausführungsform ist jedoch teuer und aufwendig, da die Vermittlungsstellen selbst umgebaut werden müßten.

Ein kostengünstigerer Weg, der mit einem geringeren Aufwand erreichbar ist, besteht darin, ausgehend von bereits vorhandenen digitalen Vermittlungsstellen eine Zusatzeinrichtung zwischen die der Vermittlungsstelle zugeordneten Netzabschlußeinrichtungen und die Vermittlungsstelle zu schalten. In dieser Zusatzeinrichtung ist für jeden zugehörigen Teilnehmeranschluß das entsprechende zweite Authentisierungs-Modul angeordnet.

Das erste Authentisierungs-Modul eines bestimmten Anschlußinhabers ist zweckmäßigerweise in der dem Teilnehmeranschluß zugeordneten Netzabschlußeinrichtung selbst angeordnet. In diesem Fall genügt ein einziges Authentisierungs-Modul, auch wenn der Inhaber eines Teilnehmeranschlusses über einen S_0-Bus bis zu acht Datenendgeräte an die Netzabschlußeinrichtung angeschlossen hat. Es ist durchaus möglich, jedes Datenendgerät, das einer Netzabschlußeinrichtung zugeordnet ist, mit einem eigenen Authentisierungs-Modul und einem eigenen Identitätsträger auszurüsten. Eine weitere Alternative kann darin bestehen, zwischen jedes Datenendgerät und der zugehörigen Netzabschlußeinrichtung eine Sicherungs-Einrichtung anzuschließen, die das jeweilige Authentisierungs-Modul enthält. Es ist jedoch leicht einzusehen, daß die beiden letztgenannten Implementierungsmöglichkeiten aufwendig und teuer sind, da für jedes Datenendgerät sowohl ein eigenes Authentisierungs-Modul als auch ein anschlußspezifischer Identitätsträger erforderlich sind. Die zur Authentisierung des Teilnehmeranschlusses zwischen den beiden Authentisierungs-Modulen auszutauschenden Informationen enthalten zum einen die Adresse eines bestimmten Teilnehmeranschlusses, eine Befehlssequenz, die z. B. in der Aufforderung an das erste Authentisierungs-Modul besteht, die ankommenden Informationen zu verschlüsseln, und eine Zufallszahl. Handelt es sich bei dem digitalen Kommunikationsnetz um ein ISDN-Netz, so erfolgt der Austausch der zur Authentisierung dienenden Informationen zwischen dem ersten Authentisierungs-Modul und dem zweiten Authentisierungs-Modul über den D-Kanal des ISDN-Netzes. Jeder Identitätsträger kann einen individuellen, auf den Inhaber des Teilnehmeranschlusses bezogenen kryptografischen Schlüssel speichern. Der Identitätsträger kann eine Chipkarte sein, die vom Inhaber eines Teilnehmeranschlusses in das erste Authentisierungs-Modul und von einer Bedienperson des Netzbetreibers in das zweite Authentisierungs-Modul einführbar sind. Eine zweckmäßige Alternative betrifft ein Software-Modul als Identitätsträger, der austauschbar in das jeweilige Authentisierungs-Modul eingesetzt werden kann. Bei einer vorteilhaften Weiterbildung kann das erste Authentisierungs-Modul zusätzlich vertrauliche Verbindungsaufbau- und/oder Serviceinformationen verschlüsseln und das zweite, der Vermittlungsstelle zugeordnete Authentisierungs-Modul die so verschlüsselten Informationen wieder entschlüsseln.

Da die Verbindungsaufbau- und/oder Service-Informationen eine höhere Bitrate benötigen als die Authentisierungs-Informationen, ist es zweckmäßig, zu den ersten und zweiten Authentisierungs-Modulen jeweils ein separates kryptographisches Modul zu installieren, in dem Identitätsträger eingesetzt werden können, die ausschließlich die Verbindungsaufbau- und/oder Service-Informationen ver- und/oder entschlüsseln.

Die Erfindung wird nachstehend anhand der Ausführungsformen in Verbindung mit den beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 in schematischer Weise einen Ausschnitt eines digitalen Kommunikationsnetzes, das den Verbindungsweg von einem Fernsprechapparat zu einer digitalen Vermittlungsstelle zeigt, in dem die Erfindung verwirklicht ist,

Fig. 2 eine zweite Ausführungsform, bei der die erfindungsgemäßen Authentisierungs-Module auf der Seite der Vermittlungsstelle in einer Zusatzeinrichtung eingebaut sind,

Fig. 3 ein detailliertes Blockschaltbild der Netzabschlußeinrichtung mit dem erfindungsgemäßen Authentisierungs-Modul und

Fig. 4 ein detailliertes Blockschaltbild einer anschlußspezifischen Baugruppe der Vermittlungsstelle mit ei-

nem eingebauten Authentisierungs-Modul.

Fig. 5 das Rahmenformat der ISDN-Bitströme.

Fig. 1 zeigt in vereinfachter Darstellung einen Teil eines digitalen Kommunikationsnetzes, das für die nachfolgende beispielhafte Beschreibung ein ISDN-Netz sein soll. Teilnehmerseitig ist als Datenendeinrichtung ein Fernsprechapparat 20 dargestellt, der über einen S_0-Bus 25 mit einer Netzabschlußeinrichtung 10 verbunden ist. Die Netzabschlußeinrichtung 10, auch Net Terminator (NT) genannt, kann in dem Gebäude oder Raum eines Teilnehmer-Anschluß-Inhabers installiert sein. An den S_0-Bus 25 können bis zu acht Datenendeinrichtungen, wie z. B. weitere Fernsprechapparate 20, Facsimilegeräte oder Personalcomputer, angeschlossen werden. In dem erläuterten Beispiel ist ein erfindungsgemäßes Authentisierungs-Modul 40 in die Netzabschlußeinrichtung 10 eingebaut, in das ein Identitätsträger 50 eingesetzt sein kann. Bei dem Identitätsträger 50 kann es sich um eine Chipkarte oder um ein Software-Modul handeln. Das Authentisierungs-Modul 40 und der Identitätsträger 50 sind derart ausgelegt, daß sie Informationen zur Authentisierung eines bestimmten Teilnehmers mit einem teilnehmerspezifischen oder anschlußspezifischen Schlüssel verschlüsseln oder entschlüsseln können. Dieser Schlüssel kann in einem Speicherbaustein der Chipkarte des Anschlußinhabers abgelegt sein. Die Netzabschlußeinrichtung 10 ist ausgangsseitig in bekannter Weise über eine verdrillte Zweidraht-Leitung mit einer ihr zugewiesenen ISDN-Vermittlungseinrichtung 30 verbunden. Es ist selbstverständlich, daß ein ISDN-Netz mehrere Netzabschlußeinrichtungen 10 und mehrere Vermittlungssysteme 30 umfaßt, die über verdrillte Zweidraht-Leitungen untereinander verbunden sein können. In Zukunft werden die herkömmlichen Zweidraht-Leitungen beispielsweise durch Glasfaser-Kabel ergänzt und ersetzt. Die Vermittlungseinrichtung 30 enthält mehrere Baugruppen 80 (in Fig. 1 ist lediglich eine anschlußspezifische Baugruppe 80 dargestellt), die bestimmten Teilnehmeranschluß-Inhabern zugeordnet sind. Gemäß der ersten erfindungsgemäßen Ausführungsform ist ein Authentisierungs-Modul 60 in jeder anschlußspezifischen Baugruppe 80 angeordnet, in das eine teilnehmerbezogene Chipkarte oder ein anschlußspezifisches Software-Modul 70 im Bedarfsfall von einer Bedienperson eingesetzt wird. Es sei angenommen, daß der Identitätsträger 70 in der Vermittlungseinrichtung 30 ebenfalls den individuellen kryptographischen Schlüssel des Anschlußinhabers für den Fernsprechapparat 20 enthält. Der genaue Ablauf einer Authentisierung des Teilnehmers des Fernsprechapparates 20 gegenüber der Vermittlungseinrichtung 30 wird weiter unten noch genauer erläutert.

In Fig. 2 ist eine alternative Ausführungsform dargestellt, bei der eine Zusatzeinrichtung 100 zwischen die Netzabschlußeinrichtung 10 und die Vermittlungseinrichtung 30 geschaltet ist. Der besseren Übersichtlichkeit wegen zeigt Fig. 2 die Zusatzeinrichtung 100 nur mit dem eingebauten Authentisierungs-Modul 60. Normalerweise sind in der Zusatzeinrichtung 100 alle Authentisierungs-Module installiert, die den Teilnehmern oder Netzabschlußeinrichtungen zugeordnet sind, die allesamt von der Vermittlungsstelle 30 bedient werden. Die Anschlußleitungen sind hierzu in den Fig. 1 und 2 angedeutet. Wiederum können die Identitätsträger 70 als Chipkarte von außen von einer Bedienperson eingeführt werden, oder aber bereits bei der Implementierung als Software-Modul in das jeweilige Authentisierungs-Modul 60 eingesetzt werden. Die Zusatzeinrichtung 100 hat den Vorteil, daß bereits vorhandene Vermittlungsstellen des ISDN-Netzes weiterhin benutzt werden können, ohne zeitaufwendige, teure und komplizierte Änderungen an den Vermittlungssystemen vornehmen zu müssen, um eine Authentisierung beispielsweise des Teilnehmers des Fernsprechapparates 20 gegenüber der Vermittlungseinrichtung 30 durchführen zu können.

Fig. 3 zeigt ein vereinfachtes Blockschaltbild der bekannten Netzabschlußeinrichtung 10, in die das erfindungsgemäße Authentisierungs-Modul 40 zusammen mit dem Identitätsträger 50 installiert ist. Teilnehmerseitig besitzt die Netzabschlußeinrichtung 10 eine Anschlußeinheit für den S_0-Bus 25, an den bis zu acht Datenendeinrichtungen 20 anschließbar sind. Da der Aufbau und die Funktionsweise der Netzabschlußeinrichtung 10 allgemein bekannt ist, werden nachfolgend nur die wesentliche Baugruppen kurz erläutert. Grundsätzlich weist die Netzabschlußeinrichtung 10 einen Sendepfad und einen Empfangspfad auf. Der Sendepfad umfaßt einen Codierer 210, der den abgehenden Datenstrom nach bekannten Codierverfahren moduliert, einen Multiplexer 200, der die Aufgabe hat, die beiden B-Kanäle und den D-Kanal im Zeitmultiplexverfahren zu einem zusammenhängenden Datenstrom zusammenzusetzen. Ein entsprechendes Rahmenformat besteht aus 48 Bits pro 250 ms, wobei lediglich vier D-Kanalbits pro Rahmen vorgesehen sind. Mit anderen Worten werden über den D-Kanal 16 kBit/s übertragen. Wie nachfolgend noch erläutert wird, erfolgt die Authentisierung eines Teilnehmers gegenüber der Vermittlungseinrichtung 30 über diesen D-Kanal. Der Sendepfad verläuft danach nacheinander über einen Sender 180 zu einem Gabelumschalter 170, der den abgehenden Datenstrom auf eine Zweidrahtleitung gibt, die die Vermittlungsstelle 30 mit der Netzabschlußeinrichtung 10 verbindet. Ankommende Datenströme durchlaufen die Gabelschaltung 170, einen Empfänger 160 und eine Einrichtung 150, die den empfangenen Datenstrom entzerrt, verstärkt und aus diesem das Taktsignal rückgewinnt. Als nächstes durchläuft der Datenstrom einen Demultiplexer 140, der den Datenstrom wieder in die beiden B-Kanäle und den D-Kanal zerlegt. Der demultiplexierte Datenstrom durchläuft einen Decodierer 130 und wird anschließend entsprechend einer Zieladresse über den S_0-Bus 25 beispielsweise zu dem Fernsprechapparat 20 übertragen. Eine Echokompensation 190, die parallel zwischen den Sender 180 und den Empfänger 160 geschaltet ist, dient unter anderem dazu, abgehende Nachrichten, die über den Gabelumschalter 170 und den Empfänger 160 dem Empfangspfad zugeführt werden, zu kompensieren. Das Herzstück der Netzabschlußeinrichtung 10 ist eine Steuereinheit 220, die die Verwaltung und Steuerung der einzelnen Baugruppen miteinander steuert. Das erfindungsgemäße Authentisierungs-Modul 40 mit dem eingesetzten Identitätsträger 50 ist beispielsweise mit der Steuereinheit 220, dem Codierer 210, dem Multiplexer 200, dem Demultiplexer 140 und dem Decodierer 130 verbunden. Die Steuereinheit 220 hat ferner die Aufgabe, die Authentisierungseinrichtung, d. h. das Authentisierungs-Modul 40 und den Identitätsträger 50, je nach Situation zu aktivieren oder zu deaktivieren.

In Fig. 4 ist beispielsweise das vereinfachte Blockschaltbild einer teilnehmerspezifischen Baugruppe 80 dargestellt, die in der Vermittlungseinrichtung 30 installiert ist. Die anschlußspezifische Baugruppe 80 bildet im wesentlichen das Gegenstück zu der Netzabschlußein-

richtung 10. Ankommende Datennachrichten gelangen über die Zweidraht-Leitung zu einem Gabelumschalter 230 und durchlaufen anschließend einen Demultiplexer 240, einen Decoder 250 und einen D-Kanal-Händler 260. Der D-Kanal-Händler 260 versorgt eine zentrale Steuereinheit der Vermittlungseinrichtung 30 mit den entsprechenden Steuerinformationen. In umgekehrter Richtung laufen abgehende Nachrichten über einen Codierer 270, über einen Multiplexer 290 und über den Gabelumschalter 230 auf die Zweidraht-Leitung zur Netzabschlußeinrichtung 10. Auch in der anschlußspezifischen Baugruppe 80 übernimmt eine Steuereinheit 280 die Verwaltung und das Zusammenspiel der einzelnen Bauelemente. Erfindungsgemäß ist das Authentisierungs-Modul 60 mit einer von außen einführbaren Chipkarte oder einem eingesetzten Software-Modul 70 in der anschlußspezifischen Baugruppe 80 installiert. Die Authentisierungseinrichtung 60, 70, die das Authentisierungs-Modul 60 und den Identitätsträger 70 umfaßt, ist wiederum mit dem Codierer 270, dem Decoder 250, dem D-Kanalhändler 260 und der Steuereinheit 280 verbunden. Wie bereits erwähnt, kann die Authentisierungseinrichtung 60, 70 auch in der Zusatzeinrichtung 110 installiert sein, wie dies in Fig. 2 dargestellt ist.

Es ist zwar zweckmäßig, die Authentisierungseinrichtung 40, 50 (das Authentisierungs-Modul 40 und den Identitätsträger 50) in der Netzabschlußeinrichtung 10 selbst unterzubringen, da auf diese Weise unabhängig von der Anzahl der angeschlossenen Datenendeinrichtungen 20 lediglich eine einzige Authentisierungseinrichtung 40, 50 erforderlich ist. Allerdings ist es auch denkbar, die teilnehmerseitige Authentisierungseinrichtung 40, 50 in jeder Datenendeinrichtung 20 anzuordnen. Eine weitere Alternative besteht darin, zwischen die Netzabschlußeinrichtung 10 und jedes angeschlossene Datenendgerät 20 eine nicht dargestellte Sicherungs-Einrichtung vorzusehen, in der die Authentisierungseinrichtung 40, 50 implementiert ist. Die beiden letztgenannten Möglichkeiten führen aber zu dem wesentlichen Nachteil, daß ein Teilnehmer für jede Datenendeinrichtung 20, die er an seine Netzabschlußeinrichtung 10 anzuschließen wünscht, eine separate Authentisierungseinrichtung 40, 50 mitkaufen müßte. Aus wirtschaftlichen Gründen ist es zweckmäßig, Authentisierungseinrichtungen 40, 50, wie in Fig. 1 dargestellt, in der Netzabschlußeinrichtung 10 selbst zu installieren. Der Identitätsträger 50 kann in Form eines Software-Moduls von dem Netzbetreiber bei der Installation der Netzabschlußeinrichtung 10 bei dem Teilnehmer eingesetzt werden. Handelt es sich bei dem Identitätsträger 50 um eine Chipkarte, so kann der Teilnehmer diese Chipkarte, die seinen individuellen Teilnehmerschlüssel enthält, z. B. beim Netzbetreiber erwerben.

Es wird nunmehr detaillierter auf die Authentisierung des Teilnehmers des Fernsprechapparates 20 gegenüber der Vermittlungsstelle 30 eingegangen.

Es sei angenommen, daß eine teilnehmerseitige Authentisierungseinrichtung 40, 50 in der Netzabschlußeinrichtung 10 und eine zweite Authentisierungseinrichtung 60, 70 in der dem bestimmten Teilnehmer zugeordneten Baugruppe 80 in der Vermittlungsstelle 30 installiert sind. Gemäß der in Fig. 2 gezeigten Ausführungsform kann die Authentisierungs-Einrichtung 60, 70 auch in der Zusatzeinrichtung 110 installiert sein. Die nachfolgend beschriebenen Verfahren laufen für beide Ausführungsformen im wesentlichen in gleicher Weise ab.

Es sei nun der Fall angenommen, daß der Teilnehmer den Hörer seines Fernsprechapparates 20 abnimmt, um einen Verbindungswunsch anzukündigen. Daraufhin sendet der Fernsprechapparat 20 über die Netzabschlußeinrichtung 10 eine Verbindungsaufbau-Nachricht an die Vermittlungseinrichtung 30. Unter Ansprechen auf die Verbindungsaufbau-Nachricht schickt die Vermittlungseinrichtung 30 eine Verbindungsaufbau-Bestätigungsnachricht zur Netzabschlußeinrichtung 10 zurück. Zusätzlich werden Authentisierungs-Informationen von der Vermittlungseinrichtung 30 zur Netzabschlußeinrichtung 10 übertragen. Diese Authentisierungs-Informationen können Adreßdaten des Teilnehmers des Fernsprechapparates 20, Befehlsdaten und Informationsdaten enthalten. Die Befehlsdaten enthalten z. B. für die Authentisierungseinrichtung 40, 50 in der Netzabschlußeinrichtung 10 die Aufforderung "Sende empfangene Informationen verschlüsselt zurück". Die zur Authentisierung dienende Information kann beispielsweise eine Zufallszahl sein, die mindestens 8 Byte lang ist und beliebig viele Füllinformationen umfaßt. Die Steuereinheit 220 liest die empfangene Authentisierungs-Information, insbesondere die Befehlsdaten, und veranlaßt daraufhin die Authentisierungseinrichtung 40, 50 die zusammen mit der Adresse und den Befehlsdaten übertragenen Informationen mit dem teilnehmer- oder anschlußspezifischen Schlüssel zu verschlüsseln, und über den Multiplexer 200, den Sender 81, den Gabelumschalter 170 und die Zweidraht-Leitung zum Identitätsträger 70 der Vermittlungsstelle 30 zurückzusenden. Wie bereits erwähnt, werden die der Authentisierung dienenden Informationen in dem D-Kanal übertragen, der mit Hilfe des Demultiplexers 140 aus den empfangenen Daten herausgefiltert und dem Identitätsträger 50 zugeführt wird. Die verschlüsselten Informationen erreichen das Authentisierungs-Modul 60 in der teilnehmerspezifischen Baugruppe 80 der Vermittlungsstelle 30. Die Steuereinheit 280 aktiviert die Authentisierungs-Einrichtung 60, 70, um die verschlüsselte Information mit dem teilnehmerspezifischen Schlüssel, der dem Schlüssel auf dem Identitätsträger so der Netzabschlußeinrichtung 10 entspricht, zu entschlüsseln. Die Steuereinheit 280 oder die Authentisierungs-Einrichtung 60, 70 überprüft die entschlüsselte Information mit der zuvor abgesendeten Information. Stimmen die beiden Informationen überein, wird der D-Kanal-Händler 260 über die Steuereinheit 280 aktiviert und sendet eine Steuernachricht zur Zentraleinheit der Vermittlungsstelle 30, um ihr mitzuteilen, daß der, einen Verbindungsaufbau suchende Teilnehmer dazu auch berechtigt ist. Daraufhin veranlaßt die Vermittlungsstelle 30 die Netzabschlußeinrichtung 10 des Teilnehmers, Verbindungsaufbau- und Service-Informationen zu übertragen.

Eine vorteilhafte Weiterbildung sieht nun vor, die nach einer erfolgreichen Authentisierung des Teilnehmers zu übertragenden Verbindungsaufbau- und Service- Informationen ebenfalls in verschlüsselter Form beispielsweise im D-Kanal zur Vermittlungsstelle 30 zu übermitteln. Die Verschlüsselung der Verbindungsaufbau- und Serviceinformationen des Teilnehmers kann entweder die Authentisierungs-Einrichtung 40, 50 selbst oder eine zusätzliche Sicherungs-Einrichtung bestehend aus einem Sicherungs-Modul und einem Identitätsträger (nicht dargestellt) ausführen. In der Vermittlungsstelle oder in der Zusatzeinrichtung übernimmt die Authentisierungs-Einrichtung 60, 70 oder eine separate Sicherungs-Einrichtung bestehend aus einem Sicherungs-Modul und einem teilnehmerbezogenen Identitätsträger die Entschlüsselung der verschlüsselten Verbindungsaufbau- und/oder Service-Informationen. Dank

der Kombination dieser beiden Verfahren wird die Gefahr wesentlich eingeschränkt, wenn nicht sogar gänzlich beseitigt, daß Eindringlinge sich unberechtigt auf die Verbindungsleitung zwischen der Netzabschlußeinrichtung 10 und der Vermittlungsstelle 30 aufschalten und teilnehmervertrauliche Nachrichten anzapfen können, um auf Kosten des Teilnehmers die Vermittlungsstelle in nicht authorisierter Weise zu benutzen.

Ein weiteres Verfahren zur Authentisierung sieht vor, den Teilnehmer gegenüber der Vermittlungseinrichtung 30 vor Beginn des Verbindungsaufbaus zu authentisieren. Der Teilnehmer nimmt den Hörer seines Fernsprechapparates 20 ab, woraufhin die Netzabschlußeinrichtung 10 eine Verbindungsaufbau-Nachricht zur Vermittlungsstelle 30 überträgt. Statt eine Verbindungsaufbau-Bestätigungsnachricht an die Netzabschlußeinrichtung 10 zurückzusenden, veranlaßt die Vermittlungseinrichtung 30 bzw. die Zusatzeinrichtung 110 die Übertragung einer unverschlüsselten Nachricht, bestehend aus der Zieladresse eines bestimmten Teilnehmeranschlusses, einer Befehlssequenz und der zu verschlüsselnden Information. Unter Ansprechen auf die Befehlssequenz aktiviert die Steuereinheit 220 in der Netzabschlußeinrichtung 10 die Authentisierungs-Einrichtung 40, 50, die daraufhin in die im D-Kanal übertragene Information mit dem teilnehmerspezifischen kryptographischen Schlüssel verschlüsselt und, wie oben bereits beschrieben, zum Authentisierungs-Modul 60 in der Vermittlungseinrichtung 30 zurückschickt. Wiederum aktiviert die Steuereinheit 280 der Vermittlungsstelle 30 die Authentisierungs-Einrichtung 60, 70, die verschlüsselte Information mit dem ihr bekannten, teilnehmerspezifischen Schlüssel zu entschlüsseln. Stimmt die unverschlüsselt übertragene Information mit der entschlüsselten Information überein, erhält die Zentraleinheit der Vermittlungsstelle 30 über den D-Kanal-Händler 260 die Information, daß der einen Verbindungsaufbau wünschende Teilnehmer dazu berechtigt ist, und veranlaßt die Vermittlungsstelle, Verbindungsaufbau-Bestätigungsnachricht an die Netzabschlußeinrichtung 10 zu senden. Der Teilnehmer ist nunmehr gegenüber der Vermittlungsstelle authentisiert und kann nunmehr die Verbindungsaufbau- und Service-Informationen zur Vermittlungsstelle übertragen.

Gemäß einem weiteren Verfahren sendet die Authentisierungs-Einrichtung 60, 70 auf der anschlußspezifischen Baugruppe 80 der Vermittlungseinrichtung 30 in vorbestimmten, einstellbaren Zeitabständen eine Information einschließlich einer Adresse und einer Befehlssequenz an die Netzabschlußeinrichtung 10. Die Steuereinheit 220 der Netzabschlußeinrichtung 10 interpretiert die Befehlssequenz. Nach der Interpretation aktiviert die Steuereinheit die Authentisierungs-Einrichtung 40, 50, die über den D-Kanal angekommene Information gegebenenfalls zu ergänzen, mit dem individuellen, teilnehmerspezifischen Schlüssel zu verschlüsseln und an das Authentisierungs-Modul 60 in der Vermittlungsstelle 30 zurückzusenden. Die Steuereinheit 280 in der teilnehmerspezifischen Baugruppe 80 aktiviert nunmehr das Authentisierungs-Modul 60, die verschlüsselte Empfangsinformation mit dem ihr bekannten, teilnehmerspezifischen Schlüssel zu entschlüsseln. Stellt die Authentisierungs-Einrichtung 60, 70 oder die Steuereinheit 280 fest, daß die zu vergleichenden Informationen nicht übereinstimmen und damit die Identitätsprüfung negativ ist, sendet sie über den D-Kanalhändler 260 eine Mitteilung an die Zentraleinheit der Vermittlungsstelle 30, keinen Verbindungsaufbau einzuleiten. Das soeben beschriebene Verfahren kann auch dazu benutzt werden, die Berechtigung eines Teilnehmers während einer laufenden Kommunikation zu überprüfen. Sollte sich einmal ein unberechtigter Eindringling auf die Verbindungsleitung zwischen der Netzabschlußeinrichtung 10 und der Vermittlungseinrichtung 30 aufgeschaltet haben, so wird spätestens nach dem vorbestimmten, einstellbaren Zeitintervall die Authentisierungs-Einrichtung 60, 70 feststellen, daß sich ein Eindringling in die Verbindung eingeschaltet hat. Daraufhin wird die Vermittlungsstelle 30 veranlaßt, die bestehende Verbindung zu trennen.

Patentansprüche

1. Verfahren zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen (30) eines digitalen Kommunikationsnetzes mit wenigstens einer teilnehmerseitigen Netzabschlußeinrichtung (10), an die wenigstens eine Datenendeinrichtung (20) anschaltbar ist, wenigstens einem ersten, bei einem Teilnehmer angeordneten Authentisierungs-Modul (40), das einen ersten Identitätsträger (50) aufnehmen kann, und wenigstens einem zweiten, der Vermittlungsstelle (30) zugeordneten Authentisierungs-Modul (60), das einen zweiten Identitätsträger (70) aufnehmen kann, mit folgenden Verfahrensschritten:
Austauschen von Informationen zwischen dem ersten und zweiten Authentisierungs-Modul (40, 60), Ver- und Entschlüsseln der Informationen mit einem teilnehmerspezifischen, kryptographischen Schlüssel durch das erste Authentisierungs-Modul (40), Ver- und Entschlüsseln der Information mit dem teilnehmerspezifischen, kryptographischen Schlüssel durch das zweite Authentisierungs-Modul (60), um eine einseitige und/oder gegenseitige Authentisierung zwischen dem Teilnehmer und der Vermittlungsstelle (30) zu erhalten.

2. Verfahren zur Authentisierung nach Anspruch 1, dadurch gekennzeichnet,
daß das zweite Authentisierungs-Modul (60) in vorbestimmten, einstellbaren Zeitabständen die Information an das erste Authentisierungs-Modul (40) sendet,
daß das erste Authentisierungs-Modul (40) die empfangenen Informationen mit dem teilnehmerspezifischen Schlüssel verschlüsselt und zum zweiten Authentisierungs-Modul (60) zurücksendet,
daß das zweite Authentisierungs-Modul (60) die verschlüsselte Information unter Verwendung des teilnehmerspezifischen Schlüssels entschlüsselt und bei positiver Authentisierung des Teilnehmers die jeweilige Vermittlungsstelle veranlaßt, Verbindungsaufbauund/oder Service- Informationen anzufordern.

3. Verfahren zur Authentisierung nach Anspruch 1, dadurch gekennzeichnet,
daß die Datenendeinrichtung (20) über die Netzabschlußeinrichtung (10) ein Verbindungsaufbau-Signal zur Vermittlungsstelle (30) sendet,
daß das zweite Authentisierungs-Modul (60) unter Ansprechen auf das Verbindungsaufbau-Signal eine Information an das erste Authentisierungs-Modul (40) sendet,
daß das erste Authentisierungs-Modul (40) die Information mit dem teilnehmerspezifischen Schlüssel verschlüsselt und zum zweiten Authentisie-

rungs-Modul (60) zurücksendet,
daß das zweite Authentisierungs-Modul (60) die verschlüsselten Informationen mit dem teilnehmerspezifischen Schlüssel entschlüsselt und bei positiver Authentisierung des Teilnehmers die zugeordnete Vermittlungsstelle (30) veranlaßt, ein Verbindungsaufbau-Bestätigungssignal an die Netzabschlußeinrichtung (10) zu senden.

4. Verfahren zur Authentisierung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß nach einem Verbindungsaufbau zwischen der Netzabschlußeinrichtung (10) und der Vermittlungsstelle (30) die Authentizität des Teilnehmers zyklisch überprüft wird.

5. Verfahren zur Authentisierung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die zur Authentisierung dienenden Informationen über den D-Kanal eines ISDN-Netzes übertragen werden.

6. Vorrichtung zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen (30) eines digitalen Kommunikationsnetzes mit wenigstens einer teilnehmerseitigen Netzabschlußeinrichtung (10), an die wenigstens eine Datenendeinrichtung (20) anschaltbar ist, dadurch gekennzeichnet,
daß bei jedem Teilnehmer wenigstens ein erstes Authentisierungs-Modul (40) angeordnet ist, das einen ersten Identitätsträger (50) aufnehmen kann,
daß in der Vermittlungsstelle (30) wenigstens ein zweites Authentisierungs-Modul (60) angeordnet ist, das einen zweiten Identitätsträger (70) aufnehmen kann,
wobei die Authentisierungs-Module (40, 60) eine Information mit einem individuellen, teilnehmerspezifischen Schlüssel zur einseitigen und/oder gegenseitigen Authentisierung ver- und/oder entschlüsseln und die Informationen untereinander austauschen können.

7. Vorrichtung zur Authentisierung nach Anspruch 6, dadurch gekennzeichnet, daß die Vermittlungsstelle (30) mehrere anschlußspezifische Baugruppen (80) enthält, in der jeweils das zweite Authentisierungs-Modul (60) integriert ist.

8. Vorrichtung zur Authentisierung von Teilnehmern gegenüber einer oder mehreren Vermittlungsstellen (30) eines digitalen Kommunikationsnetzes mit wenigstens einer teilnehmerseitigen Netzabschlußeinrichtung (10), an die wenigstens eine Datenendeinrichtung (20) anschaltbar ist, dadurch gekennzeichnet, daß bei jedem Teilnehmer wenigstens ein erstes Authentisierungs-Modul (40) angeordnet ist, das einen ersten Identitätsträger (50) aufnehmen kann, daß zwischen die der Vermittlungsstelle (30) zugeordneten Netzabschlußeinrichtungen (10) und die Vermittlungsstelle (30) eine Zusatzeinrichtung (100) geschaltet ist, in der wenigstens ein zweites Authentisierungs-Modul (110) angeordnet ist, das einen zweiten Identitätsträgers (120) aufnehmen kann, wobei die Authentisierungs-Module (40, 60) eine Information mit einem teilnehmerspezifischen Schlüssel zur einseitigen und/oder gegenseitigen Authentisierung ver- und/oder entschlüsseln und die Information untereinander austauschen können.

9. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, daß in jeder an die Netzabschlußeinrichtung (10) anschaltbaren Datenendeinrichtung (20) das erste Authentisierungs-Modul (40) angeordnet ist.

10. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, daß zwischen jeder Datenendeinrichtung (20) des Teilnehmers und der zugehörigen Netzabschlußeinrichtung (10) eine Sicherungs-Einrichtung geschaltet ist, die wenigstens ein erstes Authentisierungs-Modul (40) enthält.

11. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, daß das erste Authentisierungs-Modul (40) in der Netzabschlußeinrichtung (10) angeordnet ist.

12. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 11, dadurch gekennzeichnet, daß die zwischen dem ersten und zweiten Authentisierungs-Modul (40, 60) auszutauschenden, der Authentisierung dienenden Informationen die Adresse eines Teilnehmeranschlusses, eine Befehlssequenz und eine Zufallszahl enthalten.

13. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 12, dadurch gekennzeichnet, daß das digitale Kommunikationsnetz ein ISDN-Netz ist und der Austausch der zur Authentisierung dienenden Informationen zwischen dem ersten Authentisierungs-Modul (40) und dem zweiten Authentisierungs-Modul (60) über den D-Kanal des ISDN-Netzes erfolgt.

14. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 13, dadurch gekennzeichnet, daß die Identitätsträger (50, 70) eine Chipkarte oder ein Software-Modul sind.

15. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 14, dadurch gekennzeichnet, daß das erste Authentisierungs-Modul (40) vertrauliche Verbindungsaufbau- und/oder Serviceinformationen verschlüsseln und das zweite Authentisierungs-Modul (60) die verschlüsselten Verbindungsaufbau- und/oder Serviceinformationen entschlüsseln kann.

16. Vorrichtung zur Authentisierung von Teilnehmern nach einem der Ansprüche 6 bis 14, dadurch gekennzeichnet, daß separat zu jedem ersten und zweiten Authentisierungs-Modul (40, 60) ein Sicherungs-Modul installierbar ist, das einen Identitätsträger aufnehmen und die Verbindungsaufbau- und/oder Serviceinformation verbzw. entschlüsseln kann.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 195 21 484 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 19. Dezember 1996

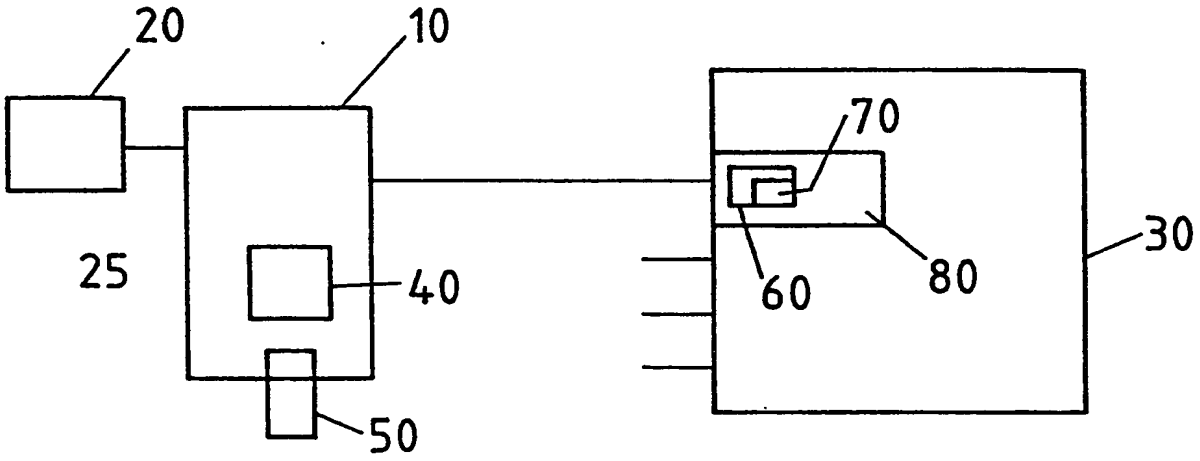


Fig. 1

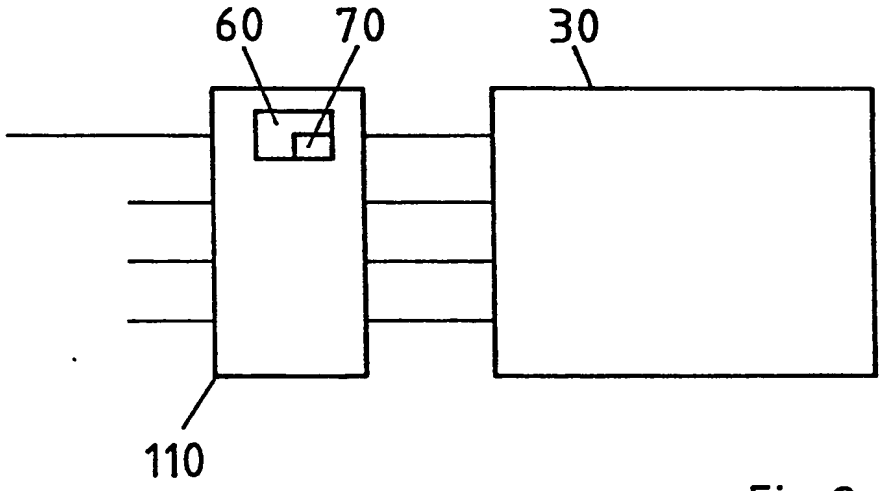


Fig. 2

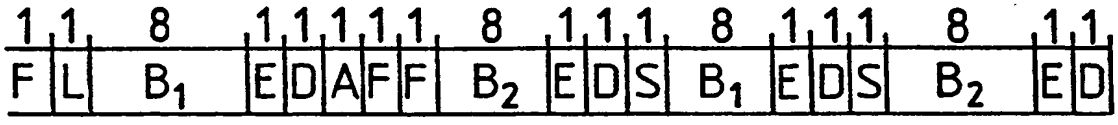


Fig. 5

Nummer: DE 195 21 484 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 19. Dezember 1996

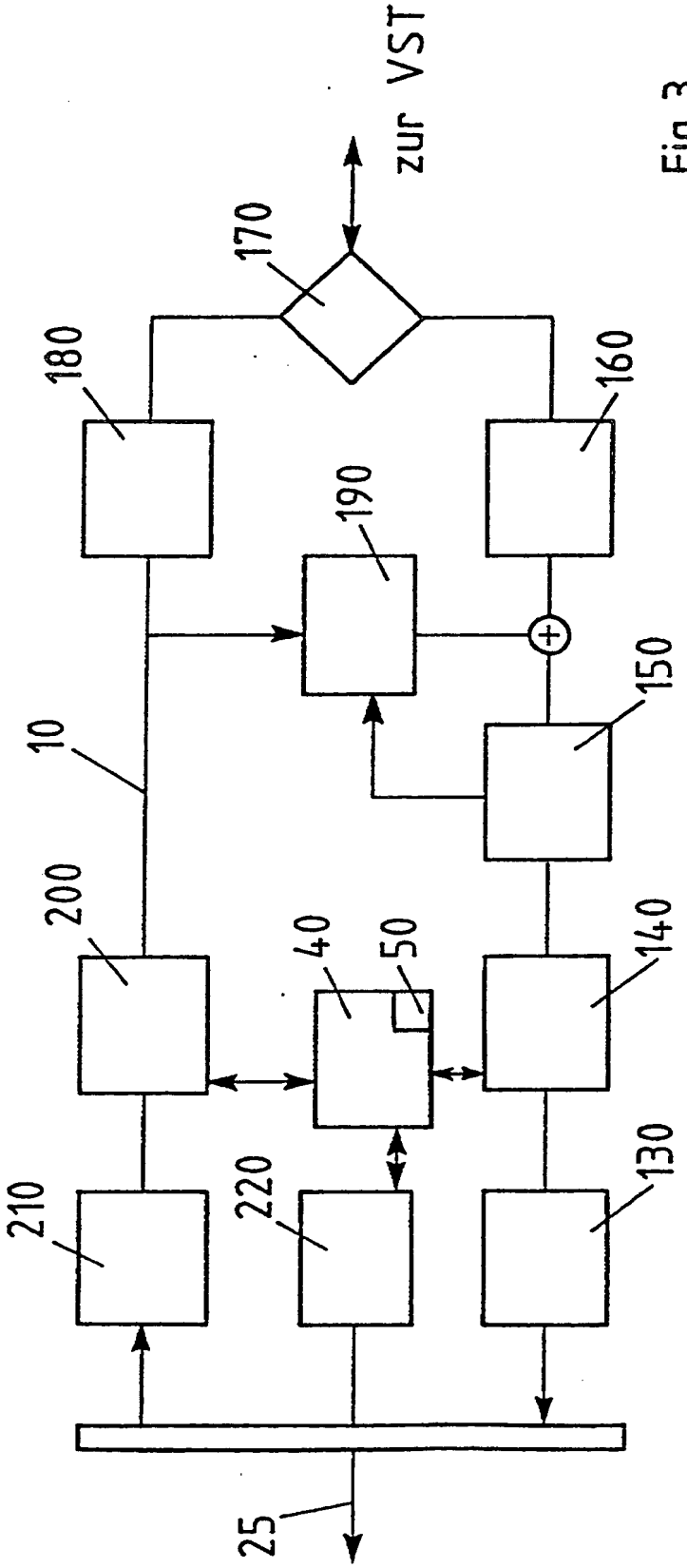


Fig. 3

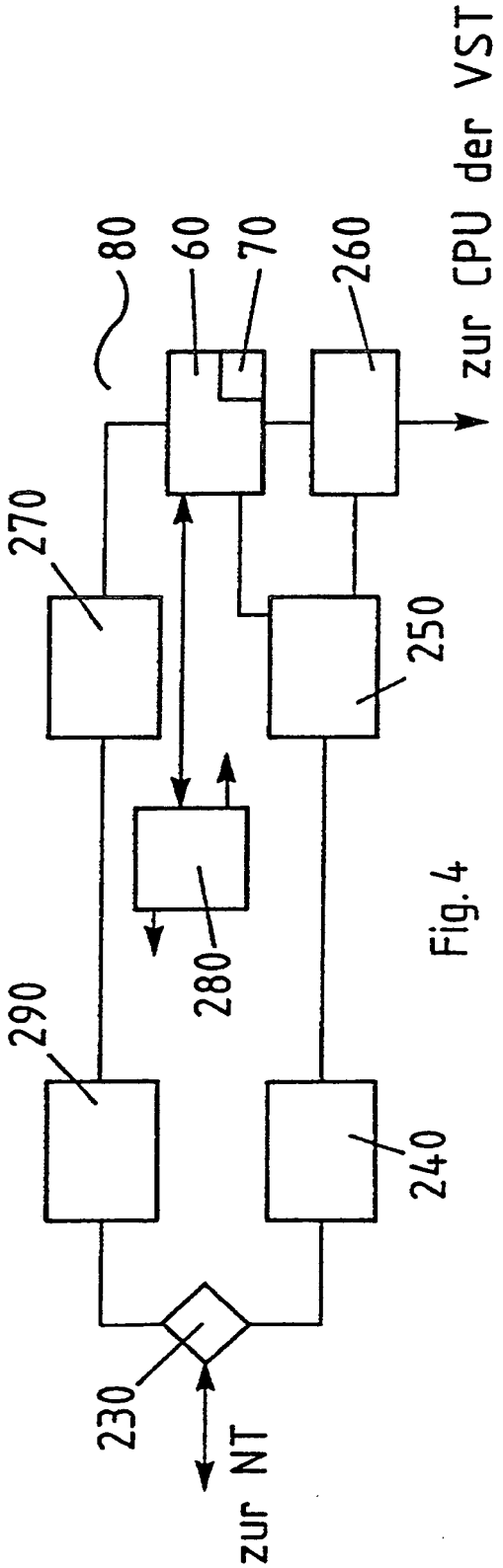


Fig. 4